DELAWARE HOMELAND SECURITY THREAT LEVEL

Homeland Security Advisory System

SEVERE
Severe Risk of Terrorist Attacks

HIGH
High Risk of Terrorist Attacks

ELEVATED
Significant Risk of Terrorist Attacks

GUARDED
General Risk of Terrorist Attacks

LOW
Low Risk of Terrorist Attacks

www.homelandsecurity.gov
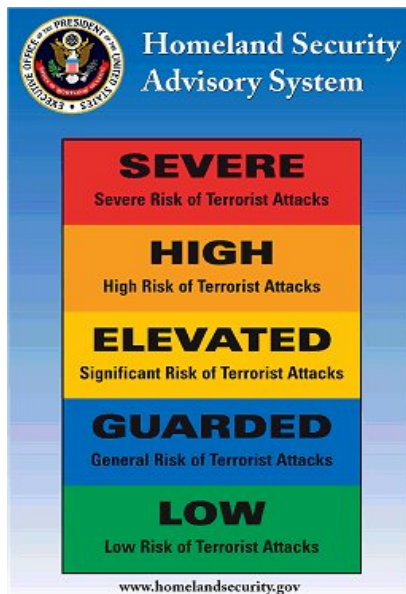
GUIDELINES

Recommended Actions for Individuals, Families, Communities, Schools, Businesses and Government

GREAT SEAL OF THE STATE OF DELAWARE · 1793 · 1847 · 1907 ·
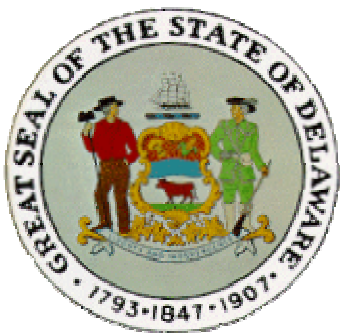
USER'S GUIDE

PURPOSE: The Homeland Security Threat Level Guideline is designed to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to the authorities and the people of the State of Delaware. This system is closely modeled on the federal Homeland Security Advisory System. It consists of warnings and instructions in the form of a set of graduated Threat Conditions that would increase as the risk of the threat increases. At each condition, individuals and organizations would implement a corresponding set of "Recommended Actions" to further reduce vulnerability or increase response capability during a period of heightened alert.

This system is intended to create a common vocabulary, context, and structure for an ongoing discussion about the nature of the threats confronting Delaware, and the appropriate protective measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private persons at home and at work.

DESCRIPTION: There are five Threat Conditions each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

Low = Green	Guarded = Blue	Elevated = Yellow	High = Orange	Severe = Red

The higher the Threat Condition, the greater the risk of terrorist attack. Risk is a function of the probability of an attack corresponding to the potential gravity of its effects. Threat Conditions shall be assigned by the Secretary of the Delaware Department of Safety and Homeland Security in consultation with the Governor's Homeland Security Advisor and the Director of the Delaware Emergency Management Agency, integrating a variety of considerations. This integration will rely on calculated assessment of risk, based on the quality of the threat information. This quality is based on (but not limited to) the credibility and degree of corroboration of the threat information. Threat Conditions may be assigned for the entire State, or they may be set for a particular geographic area or industrial sector. Assigned Threat Conditions shall be reviewed at regular intervals to determine whether adjustments are warranted. Note that the assignment of a high Threat Condition does not guarantee that a terrorist attack will occur, and the assignment of a low condition does not guarantee that an event will not occur. These conditions are only indicators of risk.

The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Recommended Actions. These are specific steps individuals, families, communities, schools, business and government organizations should take to reduce vulnerability or increase the ability to respond during a period of heightened alert. An "X" marked in a column to the right of a Recommended Action indicates its recommended implementation by individuals and families, communities, schools, business or government. Each recommended action has been assigned a numerical corresponding Action Code for reference in the event public announcements are made particular to that action. They have also been grouped by like functions into six categories: Administration & Personnel; Intelligence & Security; Plans, Operations & Training; Logistics, Facilities, Supply Transportation; Communications & Data Processing; Public Relations.

In addition to the actions listed, individuals and organizations are strongly encouraged to supplement their own individual steps particular or uniquely applicable to their activity or organization. These should be incorporated into existing plans and procedures and exercised, to facilitate a rapid, appropriate, and tailored response when needed.

INITIATING EVENT: GREEN – Low Threat

Normal operating conditions. Recommended actions when there is a low risk of terrorist attacks. In addition to the functional-specific recommended actions listed below, agencies should:
   a) Refine and exercise preplanned Protective Measures;
   b) Train on the Homeland Security Advisory System and specific preplanned Protective Measures;
   c) Regularly assess facilities and regulated sectors for vulnerabilities to terrorist attacks, and take reasonable measures to mitigate these vulnerabilities.

Action Code	Function	Recommended Action:	Individual or Family	Community	School	Business	Government
G-1	Administration and Personnel	**PLAN** – Prepare and review emergency plan to address all hazards.	X	X	X	X	X
G-2		**IDENTIFY** – Consider plans and contingencies to assist emergency worker family members. Identify and address special needs of elderly, handicapped or ill in community or workplace.	X	X	X	X	X
G-3	Intelligence and Security	**OBSERVE AND REPORT** - Report suspicious circumstances and/or individuals to law enforcement agencies.	X	X	X	X	X
G-4		**ASSESS** – Identify and regularly assess facilities for vulnerabilities.			X	X	X
G-5		**PROTECT -** Take measures to protect vulnerable assets.			X	X	X
G-6	Plans, Operations, Training	**REVIEW** – Review all plans related to the anticipation of a higher threat level. Implement as appropriate.	X	X	X	X	X
G-7		**OPERATE SAFELY** - Continue to include safety and common sense practice in daily routines.	X	X	X	X	X

Action Code	Function	Recommended Action:	Individual or Family	Community	School	Business	Government
G-8		**TRAIN** – Take first aid, Coronary-Pulmonary Resuscitation (CPR), and Automated External Defibrillator (AED) training.	X	X	X	X	X
Action Code	**Function**	**Recommended Action:**	**Individual or Family**	**Community**	**School**	**Business**	**Government**
G-9		**DESIGNATE -** Designate alternate meeting place/work sites away from home or business.	X	X	X	X	X
G-10		**COORDINATE –** Coordinate emergency plans with nearby jurisdictions / neighbors.	X	X	X	X	X
G-11	**Logistics, Facilities, Supply, Transportation**	**PREPARE AND STOCKPILE** - Prepare disaster supplies kit.	X	X	X	X	X
G-12	**Communications and Data Processing**	**IDENTITY –** Identify ways to conduct emergency notifications and communications.	X	X	X	X	X

INITIATING EVENT: BLUE – Guarded Threat

Recommended actions when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, and the functional-specific actions taken below, agencies and organizations should:
   a) Check communications with designated emergency response or command locations;
   b) Review and update emergency response procedures;
   c) Provide the public with any information that would strengthen its ability to act appropriately.

Action Code	Function	Recommended Action:	Individual or Family	Community	School	Business	Government
B-1	ONGOING	**Continue, or introduce all measures listed in Condition GREEN Advisory as needed.**	X	X	X	X	X
B-2	Intelligence and Security	**SCREEN** – Prohibit access by unauthorized persons.			X	X	X
B-3		**BRIEF** – Conduct security and safety briefings for key staff as needed.			X	X	X
B-4		**OBSERVE** - Stay alert to suspicious activity and notify the law enforcement agencies.	X	X	X	X	X
B-5		**ASSESS** – Practice safe mail-handling procedures.	X	X	X	X	X
B-6	Plans, Operations, Training	**REVIEW** – Review all plans related to the anticipation of a higher threat level. Implement as appropriate.			X	X	X
B-7		**PLAN** – Implement security plans appropriate to the facility.			X	X	X
B-8	Logistics, Facilities, Supply, Transportation	**SECURE** – Keep vehicles locked.	X	X	X	X	X
B-9		**MAINTAIN -** Check equipment and supplies. Keep vehicles fueled.	X	X	X	X	X
B-10	Communications and Data Processing	**EVALUATE** – Test communications.	X	X	X	X	X

INITIATING EVENT: YELLOW – Elevated Threat

Recommended actions when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, and the functional-specific actions taken below, agencies and organizations should:

  a) Increase surveillance of critical locations;
  b) Coordinate emergency plans as appropriate with nearby jurisdictions;
  c) Assess the precise characteristics of the threat to determine further refinement of preplanned Protective Measures;
  d) Implement appropriate contingency and emergency response plans.

Action Code	Function	Recommended Action:	Individual or Family	Community	School	Business	Government
Y-1	ONGOING	Continue, or introduce all measures listed in Conditions BLUE as needed.	X	X	X	X	X
Y-2	Administration and Personnel	**REVIEW** – Review call-back procedures for key emergency staff and scheduled leave. Consider staffing options.			X	X	X
Y-3		**IDENTIFY** – High-risk personnel and implement additional security measures as appropriate.			X	X	X
Y-4	Intelligence and Security	**SURVEY** – Increase surveillance of critical targets / facilities.		X	X	X	X
Y-5		**OBSERVE** – Routinely inspect the interior and exterior of buildings for suspicious packages.		X	X	X	X
Y-6		**INSPECT** – Visually inspect visitors and randomly inspect their suitcases, parcels and other containers.			X	X	X
Y-7		**DETERMINE** – Identify visitors' destination.			X	X	x
Y-8		**SECURE** – Lock and regularly inspect all buildings, rooms, and storage areas not in regular use.			X	X	X
Y-9		**OBSERVE** – Maintain heightened awareness of people, vehicles, and activities. Be alert to suspicious activity and report it to law enforcement agencies.	X	X	X	X	X
Y-10	Plans, Operations, Training	**REVIEW** – Review all plans related to the anticipation of a higher threat level. Implement as appropriate.	X	X	X	X	X

Action Code	Function	Recommended Action:	Individual or Family	Community	School	Business	Government
Y-11		**PATROL** - Operate random patrols to check vehicles, people and buildings.		X	X	X	X
Y-12		**REVIEW** – Meet with representatives of critical infrastructure and facilities to review contingency and evacuation plans.			X	X	X
Y-13		**ALTERNATE** – Develop and practice alternate routes to and from home/school/work.	X	X	X	X	X
Y-14	**Logistics, Facilities Supply, Transportation**	**CHECK** – Validate vendor lists for all routine deliveries and repair services. Check all deliveries to homes and facilities.	X	X	X	X	X
Y-15		**PREPARE** – Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment.	X	X	X	X	X
Y-16		**INVENTORY** – Check and replenish inventories of critical supplies and re-order if necessary.	X	X	X	X	X
Y-17		**RELOCATE** – Move or secure vehicles and objects (trash containers, crates, etc.) away from buildings.	X	X	X	X	X
Y-18		**SECURE** – Do not leave vehicles unattended. If it is necessary to leave the vehicle, lock it and check the vehicle and its chassis underside before opening the door and starting the engine.	X		X	X	X
Y-19	**Public Relations**	**COORDINATE** – Identify any planned community events where a large attendance is anticipated. Consult with event organizers regarding contingency plans, security awareness, and site accessibility and control.		X	X	X	X
Y-20	**Communications and Data Processing**	**PREPARE** – Increase the frequency of backups of critical information systems and verify availability of technical support.			X	X	X

INITIATING EVENT: ORANGE – High Threat

Recommended actions when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, and the functional-specific actions taken below, agencies and organizations should:

a) Coordinate necessary security efforts with federal, state, and local law enforcement agencies, national guard or other armed forces organizations;
b) Take additional precautions for public events, considering alternative venues or cancellation;
c) Prepare for contingency procedures, to include moving to an alternate site or dispersing the staff;
d) Restrict threatened facility access to essential personnel only.

	Function	Recommended Action:	Individual Or Family	Community	School	Business	Government
O-1	Ongoing	**Continue, or introduce all measures listed in Condition YELLOW Advisory.**	X	X	X	X	X
O-2	Administration and Personnel	**PREPARE –** Be prepared to work at an alternate site or with a dispersed workforce.	X	X	X	X	X
O-3		**ALERT** – Place all emergency management and specialized response teams on alert status. Contact all personnel to determine re-call status. Cancel scheduled leave. Ensure adequate staff coverage.			X	X	X
O-4		**PREPARE –** Be prepared for disruptions and delays of normal activities.	X	X	X	X	X
O-5	Intelligence and Security	**SECURE** – Limit visitors to those performing essential functions. Escort visitors and monitor at all times. Check where the visitors were or worked to assure nothing is amiss or left behind.			X	X	X
O-6		**BEWARE –** Exercise caution when traveling.	X	X	X	X	X
O-7		**SECURE** - Limit access points at critical facilities to essential personnel. Strictly enforce entry control procedures.				X	X
O-8		**SECURE** – Enforce parking of vehicles away from sensitive buildings. Randomly search vehicles in regulated parking areas.		X	X	X	X
O-9		**STRENGTHEN** - Increase defensive measures around key structures and events.		X	X	X	X

O-10	Plans, Operations, Training	ACTIVATE – Partially activate emergency centers with limited staffing.			X	X	X
O-11		COORDINATE – Coordinate closing public roads and facilities in order to make critical facilities less vulnerable.			X	X	X
O-12		PATROL - Increase security patrols around critical facilities.			X	X	X
O-13		CONTROL - Erect barriers and obstacles to control the flow of traffic, as appropriate. Change traffic patterns on a random basis.			X	X	X
O-14	Logistics, Facilities, Supply, Transportation	SECURE – Keep critical response vehicles in a secure area or in an indoor facility. Keep garage doors closed.			X	X	X
O-15	Public Relations	BEWARE – Take additional precautions at special events.	X	X	X	X	X

INITIATING EVENT: RED – Severe Threat

Recommended actions for severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures taken in the previous Threat Conditions, and the functional-specific actions taken below, agencies and organizations should:

    a) Increase or redirect personnel to address critical emergency needs;
    b) Mobilize, assign, and pre-position emergency response personnel, teams, and resources;
    c) Monitor, redirect or constrain transportation systems;
    d) Close public and government facilities.

Action	Function	Recommended Action:	Individual	Community	School	Business	Government
R-1	ONGOING	Continue, or introduce all measures listed in Condition ORANGE Advisory.	X	X	X	X	X
R-2	Administration and Personnel	RECALL – Implement emergency staffing.				X	X
R-3		STAFF – Fully staff Emergency Operations Center (EOC) or Command Post on a 24-hour basis. Provide security for this facility.				X	X
R-4		DESIGNATE – Assign emergency response personnel and pre-position specially trained teams. Stress the possibility of a secondary attack against first responders.				X	X
R-5		COORDINATE – Ensure 24-hour access to Chief Executive.				X	X
R-6		STAFF – Release non-critical function personnel.				X	X
R-7		STAFF – Increase or redirect personnel to protect critical facilities and infrastructure.				X	X
R-8	Intelligence and Security	SEARCH – Search all vehicles and their contents before allowing entrance to key facilities.			X	X	X
R-9		GUARD – Place an individual on watch at all key facilities 24 hours a day until the threat level has diminished.			X	X	X
R-10		IDENTIFY – Control access and implement positive identification of all personnel – no exceptions.			X	X	X
R-11	Plans, Operations, Training	RESPOND – Shelter in-place or evacuate if instructed by government officials.	X	X	X	X	X

Action	Function	Recommended Action:	Individual	Community	School	Business	Government
R-12		RESPOND – Increase defensive perimeters, including staffing, around key critical facilities. Make frequent checks of the exterior of critical facilities and parking. Begin surveillance of lower risk targets.		X	X	X	X
R-13		CONTROL - Control access routes serving key critical facilities and evacuation routes. Consider closing public roads serving key critical facilities.					X
R-14		CONTROL – Monitor, redirect or constrain transportation system.					X
R-15	Logistics, Facilities, Supply, Transportation	IDENTIFY - Make a positive identification of all vehicles located or operating within operational or mission support areas.			X	X	X
R-16		MONITOR - Increase security at water treatment facilities and increase the frequency of testing for impurities and contaminants.					X
R-17		SCREEN – Deliveries to key facilities should be approved by supervisory staff. All deliveries should be opened outside of the critical facility.				X	X
R-18		SECURE – If not already accomplished, implement parking restrictions and park vehicles away from key facilities.		X	X	X	X
R-19	Public Relations	COMMUNICATE – Contact businesses to determine operating status.	X	X	X	X	X
R-20		COORDINATE – Maintain communications with and provide security for key critical facilities.			X	X	X
R-21		PROVIDE – Provide volunteer services only if requested.			X	X	X
R-22		CLOSE – Cancel special or large events.	X	X	X	X	X
R-23		CLOSE – Close non-essential businesses.			X	X	
R-24		CLOSE – Close non-essential public and government facilities.			X		X
R-25	Communications And Data Processing	MONITOR – Listen to radio/television for current information or instructions.	X	X	X	X	X
R-26		UPDATE – Maintain and monitor emergency communications.			X	X	X
R-27		IMPLEMENT - Implement the Emergency Alert System as necessary.					X

State of Delaware

Department of Safety and Homeland Security

Revision 1, 2003

Document Control Number 450130030101